AIR WAR COLLEGE

AIR UNIVERSITY

ORGANIZING, TRAINING, AND RETAINING INTELLIGENCE PROFESSIONALS FOR CYBER OPERATIONS

by

Melissa A. Stone, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel Scott Roth

13 February 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lt Col Melissa Stone is assigned to the Air War College, Air University, Maxwell AFB, AL. Previously, she served as Commander, 35th Intelligence Squadron, 70th Intelligence, Surveillance and Reconnaissance Wing, Lackland AFB, Texas. In this capacity, she led a force of over 330 officer, enlisted, civilian, and contract personnel conducting cyberspace intelligence, surveillance and reconnaissance operations in support of Air Force, Combatant Command and National requirements.

Lieutenant Colonel Stone received her commission through the United States Air Force Academy as a Distinguished Graduate in 1998. She also received a Master of Science degree through the Air Force Institute of Technology's civilian institution program at the University of Illinois in 1999 and a Doctor of Management from the University of Phoenix in 2008.

A career intelligence officer, Lieutenant Colonel Stone has previously served as Congressional Liaison, Legislative Fellow on Capitol Hill, and Assistant Director of Operations for the White House Situation Room. She has also served in Signals Intelligence, Information Operations, analytical and training capacities and has deployed in support of several operations.

Abstract

The U.S. Department of Defense's recent growth in cyber has outpaced the Air Force's ability to adequately organize, train and retain cyber expertise. This is especially true within Air Force intelligence, a critical component of the Department's Cyber Mission Force construct and a significant contributor to the national intelligence community. To regain and retain the competitive advantage in the cyberspace domain, the Air Force must develop training tailored to each specific intelligence specialty code working in or supporting cyber operations, it must examine its organizational construct splitting the cyber force between two Major Commands, it must consider re-specialization of the 14N career field and it must examine retention mechanisms and consider options such as establishment of a Warrant Officer career field to ensure long term retention of talent.

Thesis

This study uses a qualitative approach to argue that the Air Force is currently not effectively planning for the organization, training or retention of Air Force intelligence professionals working in cyberspace operations.

Organizing, Training, and Retaining Intelligence Professionals for Cyber Operations

The digital battlefield transitioned from theory to reality at a rapid pace with a growing number of adversaries looking to the cyber domain to gain an asymmetric advantage. The traditional intelligence-gathering tradecrafts among many nations now include cyber espionage. Malicious actors, state-sponsored or not, can use network attacks to inflict significant damage on their adversaries. The extent of attacks against the U.S. is staggering; the Deputy Director of the National Security Agency (NSA), Richard Ledgett, estimates that there are “hundreds of thousands” attempted intrusions on U.S. networks each day.[1]

The Department of Defense (DoD) acknowledges this threat and has prioritized growth in cyber capabilities despite an austere budget environment. Cyber features prominently within the 2015 National Military Strategy (NMS), which highlights a growing cyber threat to U.S. interests. In response, the DoD has invested human capital into the Cyber Mission Force, a framework of national and regionally focused cyber teams under U.S. Cyber Command, with offensive and defensive capabilities.[2] The 2015 NMS recognizes people as the military’s competitive advantage and highlights the need to reward and retain technical talent.[3] The Air Force Future Operating Concept, 2015, echoes this strategy with specific goals to enhance training and modernize Airman management mechanisms within Air Force Core Mission areas, including Global Integrated Intelligence, Surveillance, and Reconnaissance (GIISR).[4]

Despite recognition of the importance of cyberspace operations and people to conduct those operations, Air Force leaders lack full understanding and appreciation for the role of intelligence in the cyber domain. The Air Force summary in DoD’s 2011 report to Congress on growing the cyber force did not include intelligence personnel.[5] In reality, Air Force intelligence personnel comprise the majority of work roles within the service’s Cyber Mission Force structure as well as within cyber exploitation and defensive operations conducted at the NSA.[6] The dual-hatted Director of NSA and Commander of Cyber Command, Admiral Rogers, noted the importance of intelligence within cyber operations when he stated “the ability of USCYBERCOM personnel to operate under delegated [Signals Intelligence] SIGINT authorities and leverage the national cryptologic platform is a critical capability… Signals intelligence information remains vital to support cyber operations.”[7] In order to fulfill the identified strategic goals in cyber, the Air Force must recognize the unique skills required for ISR in and for cyberspace and address force management appropriately. Specifically, the Air Force must examine its current organizational construct in employing ISR Airmen, it must invest in training for all ISR Air Force Specialty Codes (AFSC) in cyber operations, and it must study retention factors for these Airmen and employ novel solutions to develop and keep a competitive advantage.

Understanding the Cyber Landscape: ISR For and From Cyberspace

The 2015 DoD Cyber Strategy identifies three goals of cyber operations: defense of DoD, defense of the homeland and national interests, and support to military operations and planning.[8] To achieve these goals, Joint Publication 3-12 identifies three types of operations, Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO) and DoD Information Network (DoDIN) Operations. The Joint Publication also recognizes Computer Network Exploitation (CNE) under the oversight of the national intelligence community and Cyberspace ISR, intelligence gathering and other ISR activities to support OCO and DCO.[9] Digital Network Intelligence (DNI) describes data obtained through CNE and then analyzed.[10] These categories are often insufficient in describing the total nature of intelligence activities in the cyber domain resulting in some members of the ISR community using Cyber or Cyberspace ISR as an umbrella term.[11] A further dissection of Cyber ISR provides additional specificity.

What is Cyber ISR?

Air Force ISR expert, Colonel Matthew Hurley, suggests two main categories of Cyber ISR: ISR for and ISR from cyberspace.[12] "ISR from cyber" would include exploitation activities, such as CNE, where "ISR for cyber" would include intelligence collection and or analysis from any other source in support of cyberspace operations such as OCO or DCO.[13] Traditional SIGINT, Human Intelligence (HUMINT), or Imagery Intelligence (IMINT) collection could support cyberspace operations. As a hypothetical example, SIGINT collection could reveal an upcoming adversary military deployment or cyber-attack. This information could be used to plan OCO or DCO activities as an example of ISR for cyber. Similarly, information collected from cyber could be used in traditional kinetic operations as ISR from cyber. For instance, if an email documenting future movements of an enemy leader was collected via ISR from cyber, it could then be used to aid in kinetic targeting of that leader. All of these activities can be loosely categorized into Cyber ISR.

NSA and Cyber Command

Within the DoD the primary organizations involved in cyber are Cyber Command and its components from each of the military services, and NSA and its components from each of the services. In general, Cyber Command operates under Title 10, U.S. Code, traditional military authorities, and NSA operates under Title 50, U.S. Code, authorities including covert actions and intelligence.[14]

Cyber Command, located at Fort Meade, Maryland and collocated with the NSA, is a sub-unified command subordinate to U.S. Strategic Command. Cyber Command's mission is to plan, coordinate, integrate, synchronize and conduct activities to "direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations…"[15] Cyber Command is currently building out 133 cyber teams; National Mission Teams, Cyber Protection Teams, Combat Mission Teams and Combat Support Teams, as part of the Cyber Mission Force warfighting construct.[16] The Air Force component to Cyber Command is Air Forces Cyber (AFCYBER). Twenty-fourth Air Force Headquarters was designated AFCYBER in 2010, and designated a Joint Force Headquarters – Cyber (JFHQ-C) in 2013. Air Force Space Command is the parent Major Command (MAJCOM) of 24th Air Force. JFHQ-C serves as a command and control authority for joint cyber forces within the Cyber Mission Force.[17] As of 2014, 24th Air Force noted its manpower included over 5,400 active and 11,000 reserve personnel.[18]

The National Security Agency/Central Security Service (NSA/CSS) falls under the DoD and is a Combat Support Agency (CSA).[19] The NSA is a component of the intelligence community that employs cryptology and "coordinates, directs, and performs highly specialized activities to protect U.S. information systems and to produce foreign signals intelligence information."[20] More specifically, NSA conducts SIGINT, Information Assurance, and enables Computer Network Operations.[21] Further, NSA "is authorized to collect, process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions, and to provide signals intelligence support for the conduct of military operations."[22]

Military services provide manpower to NSA/CSS via their Service Cryptologic Components.[23] Twenty-Fifth Air Force, subordinate to Air Combat Command, has been designated as the Air Force's Service Cryptologic Component, which formalizes its relationship with NSA and makes it responsible to NSA for, "Air Force matters involving the conduct of cryptologic activities…"[24] As of 2015, 25th Air Force reported it's manpower includes nearly 30,000 active, reserve and guard personnel.[25] In addition to supplying ISR Airmen to NSA, 25th Air Force supports AFCYBER by providing ISR Airmen for the Cyber Mission Force construct under Cyber Command. Under this relationship, 25th Air Force Airmen are administratively controlled (ADCON) through their 25th Air Force unit and operationally controlled (OPCON) through AFCYBER via the JFHQ-C. This means the considerable intelligence portion of the Cyber Mission Force teams are not controlled operationally by intelligence personnel.[26] Further, with Air Force NSA/CSS forces controlled by NSA/CSS and Cyber Command controlling Air Force Cyber Mission Force forces, the Air Force retains little operational control in this domain.

Air Force Cyber Professionals

Multiple AFSCs are involved in cyber operations. In 2010, the Air Force began to restructure officer and enlisted communications career fields to prepare for growing cyberspace operations.[27] This restructuring included creation of the 17X career field for officers, which has since been even further specialized for Network Operations (17D) and Cyber Warfare Operations (17S).[28] On the enlisted side, the 3DX career field was largely morphed into various cyberspace support or communications sub-specialties. In addition, a new career field, the 1B4, was created for Network Warfare Operators.[29]

For ISR officers, there is one generalist AFSC, the 14N. This AFSC fills a variety of intelligence roles, including cyber ISR, with no additional specialization or training formally tracked.[30] For enlisted ISR personnel, almost every AFSC can play a role in Cyber ISR. The Air Force recently specialized the 1N4 analyst career field into 1N4A Digital Network Analysts, focused on ISR from cyber, and 1N4B Analysis and Production personnel.[31] In terms of practical employment, 1N3 Cryptologic Language Analysts can translate information gleaned from cyberspace and 1N0 Operations Intelligence personnel can provide cyber threat analysis and briefings supporting operations. Within the Cyber Mission Force, 1N0s fill All Source Analyst work roles, 1N3s are Language Analysts and 1N4Bs fill Target Analyst Reporter roles.[32]

For ISR from cyber, the two primary ISR specialties involved are 1N2C Signals Intelligence Analysts and 1N4A Network Intelligence Analysts, with 1N4As as the preponderance of Air Force ISR forces in both NSA and Cyber Command. Of note, per Career Field Manager policy, 1N2Cs are not eligible to fill any Cyber Mission Force work roles, limiting their career options within Cyber ISR to positions on the NSA side.[33] Both of these AFSCs require advanced training, known as the Joint Cyber Analysis Course (JCAC) prior to entering most Cyber ISR positions. In an attempt to professionalize the 1N4A career field, the HAF Career Field Manager directed that all 1N4As attend JCAC or be re-categorized as a 1N4B and lose the current 1N4A reenlistment bonus.[34]

Organizing: Current ISR Force Structure in Cyber and the Ops/Intel Debate

The nature of operations in cyberspace is dynamic and fluid. Contrary to traditional kinetic military operations, it is often difficult to characterize activity as OCO, CNE or other types of activities. Former DoD legal advisor Andru Wall notes the skills needed to collect intelligence in cyber are similar to those required to conduct an attack. Further, these operations happen quickly and transition back and forth between offensive and exploitation operations in seconds.[35] Because of this fluid nature, cyber tools may be constructed to have more than one type of capability, such as tools that can both collect intelligence when tasked and have the capability to deliver some sort of attack mechanism.[36]

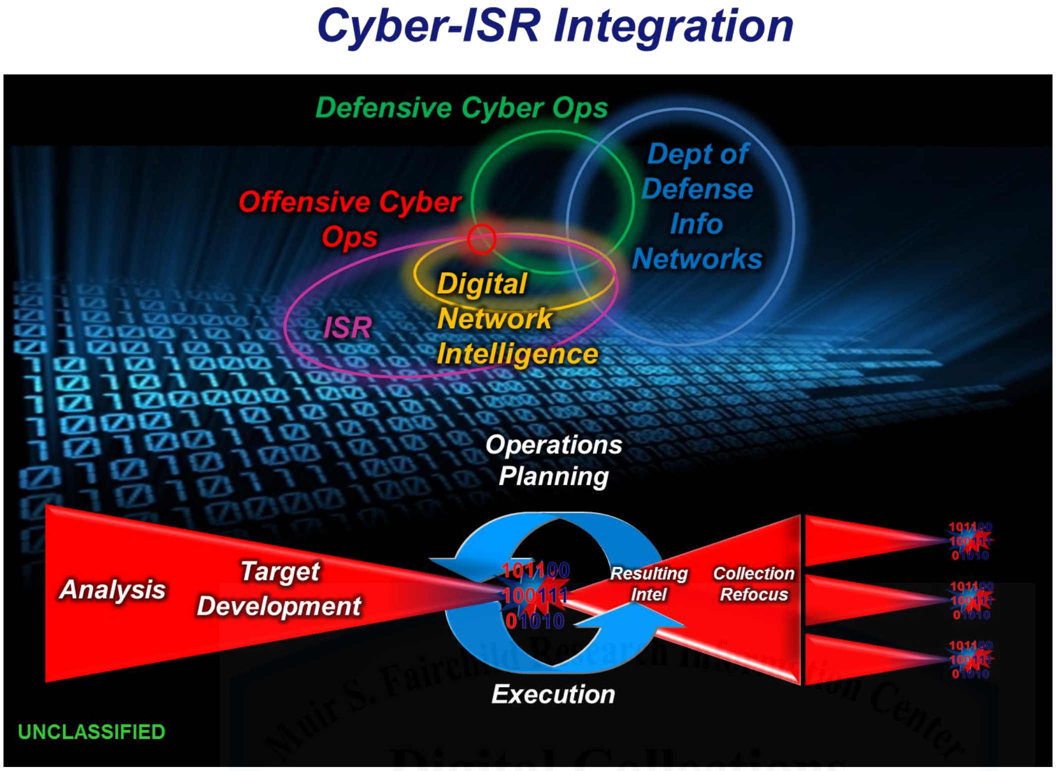

Figure 1. 25th Air Force Cyber-ISR Integration Depiction

As shown in Figure 1, 25th Air Force recognizes the dynamic nature of cyber operations and the vital role of ISR in the lead up to a potential offensive operation, in the aftermath of the operation, in analyzing results of the operation and in collecting data to drive the next operation. Depending on the nature of the target, intelligence preparation can be very difficult and lengthy. The figure also notes the relative frequency of offensive operations as minimal compared to the defensive and intelligence gathering functions.

On the national side, as discussed, Air Force personnel working in cyber mission areas at NSA are provided via 25th Air Force and operationally controlled by NSA/CSS. The same type of relationship exists within the Cyber Mission Forces, with 25th Air Force providing forces that are operationally controlled by AFCYBER for Cyber Command, despite 25th Air Force having the preponderance of forces. This team make-up highlights the critical role of intelligence, as depicted in Figure 2.[37] Cyber Mission Force team leaders, while technically fillable by 14N or 17X personnel, are overwhelmingly filled by 17X personnel with AFCYBER determining placement.[38] This organization runs the risk of creating an operations versus intelligence divide when in reality, intelligence collection is inherently a type of operation within cyberspace and may represents the bulk of operations conducted within this domain.

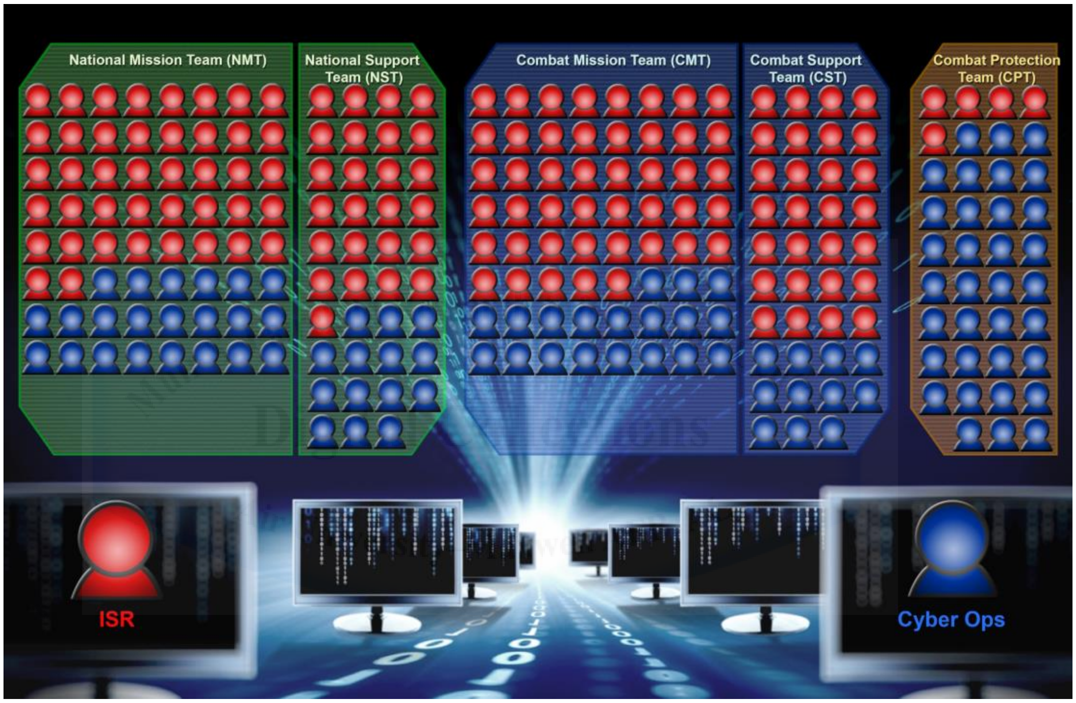
National Mission Team (NMT)
National Support Team (NST)
Combat Mission Team (CMT)
Combat Support Team (CST)
Combat Protection Team (CPT)
ISR
Cyber Ops

Figure 2. 25th Air Force Depiction of ISR and Operations Positions in Cyber Mission Force

Despite the prominent importance of ISR in cyberspace, organizationally, Cyber ISR appears to be somewhat marginalized, with 25th Air Force providing forces but retaining no operationally control, and with ISR professionals not filling Cyber Mission Force leadership roles. As noted, the two Numbered Air Forces (NAF) with cyber responsibilities are split between two MAJCOMs. Additionally, the Air Force Core Function Lead Integrator (CFLI) roles are split between MAJCOMs. The CFLI is the Air Force's primary advocate in planning, programming, and integrating activities for a core function. For ISR, the CFLI falls under Air

Combat Command while the CFLI for cyber falls under Air Force Space Command. As Hurley notes, the marginalization, or as he refers to it, the treatment of Cyber ISR as a support role, "fail[s] to recognize that ISR often *is* the mission."[39]

A recent *Foreign Policy* columnist questioned the Air Force's split cyber organization, as an outlier among the services. He noted this stove-piped structure is outdated and inefficient for modern cyber conflict.[40] Air Force Chief of Staff, General Welsh, has recognized the problems with the split organization of cyber forces and called for a single, information-focused MAJCOM. The Chief noted that creation of such a MAJCOM would take over ten years.[41]

In addition to split command chains and advocacy, plus the subordination of ISR forces to "operational" personnel, additional Secretary of the Air Force (SAF)-level actions may also increase the perceived operations vs. intelligence divide. As one example, in 2014 the SAF Chief Information Officer (CIO), changed procedures for authorizing the "Cyberspace Operations Badge," to ensure only personnel from 17X, or 1B4 AFSCs in "operations-focused" jobs could be approved for badge wear.[42] Procedures are included for other AFSCs to earn the badge, but they are significantly cumbersome; requiring individual justification through MAJCOM chains to the SAF/CIO for consideration.[43] This policy rescinded a 2010 policy awarding the badge for a larger group of personnel with cyber experience, mandating that non-17X/1B4 AFSCs wear the badge if they completed an online course and had at least one year of "cyberspace experience."[44]

Training and Tracking Expertise: Equipping ISR Professionals to Win in Cyberspace

The split organization within the Air Force's cyber community also manifests in different force management constructs for 1NX/14N and 17X/1B4 personnel, to include training, retention tools, and the ability to track and develop talent. A 2010 RAND study on cyber human capital identified the need for the Air Force to tackle this problem strategically and across all specialties, yet human capital management is still conducted within functional management stovepipes.[45]

For officer force management, Air Force Space Command established an office to track cyber experience, regardless of AFSC or organization.[46] Twenty-fifth Air Force and Air Combat Command have not established dedicated force management procedures for Cyber ISR personnel.[47]

A review of the current intelligence officer course curriculum demonstrates the wide variety of jobs 14Ns must be prepared to enter and includes only 48 hours, or less than 5% of the course time, on SIGINT and cyber combined.[48] The Air Force relies on NSA and Cyber Command for any other mission-specific training for ISR officers. In an informal survey of ISR officers in the 659th ISR Group in 2014, subjects expressed a significant gap in training between their initial Air Force intelligence training and their on-the-job or mission-specific training within the Cyber Mission Force or NSA. These members felt that many of the existing training opportunities were designed for a technical audience, such as the 17X. Specific areas that these subjects identified as gaps were networking fundamentals, network exploitation techniques, current adversary and U.S. capabilities, SIGINT requirements and reporting, and network security fundamentals. Of note, none of the 14Ns surveyed had a technical academic degree or felt that one was required if adequate training for 14Ns existed.[49]

For enlisted personnel, following initial skills training, the Air Force is reliant on JCAC and several courses offered by NSA and Cyber Command. Air Force Space Command has established its own schoolhouse for 1B and 17X personnel to provide advanced training following initial training.[50] While intelligence personnel can attend these courses, they are not part of an established 1N/14N training pipeline, 1N/14N personnel typically can only attend on a space-available basis, and these courses are not geared towards intelligence personnel without 1B/17X initial skills training. Air Force Space Command has also created a Cyber Intelligence Formal Training Unit (IFTU) for officer and enlisted ISR personnel, but this course was designed for intelligence personnel that will be assigned to Air Force Space Command cyber units, ISR for cyber, not intelligence personnel working in 25 AF units, ISR from cyber.[51] The Air Force must recognize the growing role of intelligence personnel in cyber operations and must invest in specific, tailored training for all ISR personnel.

Retaining: Preserving the Competitive Advantage

The Headquarters Air Force (HAF) ISR career field managers monitor retention data and look for trends, but only reactively. For instance, even for individuals who elect to separate from service, no formal Air Force exit interview is conducted to identify why they are leaving the service because the ISR managers feel current retention numbers do not warrant this level of study.[52] This type of analysis puts managers in the position of always being reactive in force management decisions and being uniformed of any retention decision factors that have not yet resulted in separations.

Despite the austere budget, both the 1B4 and 1N4A career fields are on the critically manned career field listing and eligible for SRBs.[53] The bonus amount may still not be enough to compete with industry cyber opportunities with jobs such as cyber security analysts who easily earn about $85,000 annually.[54] In addition to competing with industry, ISR positions in cyber are also growing within the government civilian ranks, adding another layer of competition. For instance, a cursory review of civilian jobs seeking applicants revealed several Cyber ISR positions across all services. One Army position, for a Cryptologic Cyberspace Intelligence Specialist at the GG-13 level, showed an annual salary range from $92,145 to $119,794.[55] By one accounting, an E-5 with 10 years of service time makes between $52,000 and $62,000 a year with allowances included, or with an SRB, roughly $62,000 to $75,000 for the years the bonus is paid.[56] A 2014 RAND study suggests the private sector salaries are growing even higher because of the scarcity of qualified personnel, noting qualified personnel can negotiate between companies to drive their salary and benefits higher.[57] This increased competition for skilled professionals should drive a relook into the SRB levels for Cyber ISR Airmen.

For 1N4As, as the career field was recreated in 2014, members that had already reenlisted to gain retainability to attend JCAC may not have been eligible to reenlist as a new 1N4A and take advantage of the new SRB. This could manifest in differing levels of compensation for the same work. The Air Force must reexamine these bonus procedures, and communicate them across the force and Military Personnel Flights, to ensure all 1N4As are SRB-eligible, regardless of previous enlistment contracts prior to the designation of the 1N4A AFSC.

Extended service time requirements also exist for both 1N4A and 1B4 advanced technical training, but are limited to 3 years for technical training per Air Force Instruction.[58] For instance, JCAC and the advanced cyber operations course for 1B4s each come with retainability requirements of 3 years.[59] The Air Force's current push to train all 1N4As with JCAC means a large portion of 1N4A JCAC graduates are still either within their JCAC retainability or within their service commitment from their Selective Reenlistment Bonus (SRB), and are not yet at a decision point for longer retention.[60] Looking only at current retention data will not aid managers in projecting what force management programs would be useful to retain these experts after their service commitment has expired. The HAF intelligence directorate (HAF/A2) should conduct recurring surveys of active duty Cyber ISR personnel to gather data and enable proactive decisions.

Unfortunately for ISR officers and civilians in cyber, there is not yet a fully-functioning mechanism to track their retention. The 14N career management team created a Career Path Tool (CPT) that will provide a way to track varying levels of experience within the 14N pool; this tool should be helpful if used as an assignments input to assure proper placement of 14Ns with cyber experience.[61] The HAF/A2 team should also use this data to survey 14Ns with cyber experience to determine their perspective on factors impacting their retention. The tool must also be heavily advertised as the squadron commanders interviewed were, in general, not familiar with the tool.[62]

In the absence of such data, informal interviews of intelligence squadron commanders in cyber, who are conducting exit interviews with their separating members and are engaging their members on future decisions, helps to reveal these retention factors. Initial unit-level concerns for 1NX personnel in cyber include career path and training opportunities and job satisfaction. While there is advanced training in the form of JCAC for select 1NX personnel conducting ISR from cyber operations, there is a dearth of available training for IN and 14N personnel working in ISR from and for cyber; this lack of defined training could be the source of some retention concerns the squadrons reported. Another related concern uncovered at the unit level is the unclear career path options for 1Ns in cyber and the potential that future assignments may not employ their extensive cyber skills. Commanders also noted following a lengthy formal and informal training pipeline and then finally getting operational experience, to attain the next rank individuals must eventually leave their technical positions and advance into leadership positions to be promoted.[63] RAND echoes the commanders' concerns, noting the difficulty of military organizations in building deep expertise, required in cyberspace operations, because of the desire to value breadth of experience.[64] The mention of job satisfaction is especially interesting, as the commanders noted the pace of actual operations within the new Cyber Mission Force teams has been slow while the teams train and prepare. These factors, combined with the competitive nature of the job market and inconsistent retention mechanisms, plus no first-hand data on personal retention factors, provide clear cause for concern in the long term.

Recent RAND interviews of cyber personnel echo the unit-level concerns noting their subjects reported concern about career management and utilization and the need for tailored career development and training. These subjects also noted a monetary competition from industry that was counter-balanced by the promise of a cyber-warfare mission that industry cannot provide.[65] This draw to a desirable mission was also noted by the commanders interviewed for this research paper. The commanders suggested this draw was tenuous and could be reduced if existing frustrations with career options, training and force management are not ameliorated.[66]

Recommendations

A review of current policy and recent studies as well as inputs from operational leaders leads to several recommendations within the categories of organization, training and retention in order for the Air Force to provide the best possible contribution to cyber warfare.

Organization

The need for a merged 24th and 25th Air Force under an information-focused MAJCOM is clear and acknowledged by Air Force leadership. While awaiting this new MAJCOM, HAF/A2 and 25th Air Force must continue to advocate for Cyber ISR as a core ISR mission and provide focused career field management, develop cyber training for each ISR AFSC in cyber operations and gain advocacy for Cyber ISR within the CFLI construct. In addition, the Air Force should examine the role of the JCAC-trained 1N2C and ensure this group of individuals is eligible for Cyber Mission Force positions and afforded the same incentives that the 1N4As receive.

On the officer side, the organization of the 14N career field also merits discussion. Operations in the cyber domain can be very dynamic and technical and require specifically and continually trained Airmen. With intelligence likely being the predominant type of cyber operations, 14Ns must be equipped to lead these operations. This involves development of training as discussed but should also be accompanied by a review of the career field itself. Over 650 14Ns currently work in SIGINT and cyber positions, representing almost 25% of the overall career field.[67] As discussed, these two fields are inextricably linked. The preponderance of intelligence forces within cyber operations, the natural mission linkages between cyber operations and intelligence, and the need for specific and continual training of cyber intelligence personnel lead to a recommendation to create a specialized 14N for SIGINT and cyber. If the Air Force invested in this specialization, it could develop a core of ISR professionals equipped and prepared to develop true service-specific cyber capabilities and leverage national capabilities for Air Force core mission areas.

Training and Tracking

As noted, the Air Force must invest in creation of training for each ISR AFSC involved in cyber operations. The 1N4A and 1N4B career field split should generate split technical training programs where each group can develop initial skills, prior to more advanced training, such as JCAC for the 1N4As. A cyber ISR Formal Training Unit (FTU) should be developed with courses for each ISR AFSC in cyber operations. Given the nature of cyberspace, the incorporation of Interactive Multimedia Instruction (IMI) should be explored. New Air Force trainees will be digital natives, so technology can be an advantage in their training if designed with an understanding of current educational research.[68] Further, if this type of instruction includes simulations or gaming, it could result in more cognitive gain than traditional instruction, as shown in the meta-analysis by Vogel, et al.[69]

Tracking Air Force ISR professionals with cyber expertise is another important area currently not fully optimized. Completion of JCAC allows for an administrative tracking mechanism for those graduates, but the other AFSCs, to include officers, must have a comprehensive mechanism to track cyber skills and experience. HAF's CPT provides a promising option if this tool is used in assignment decisions and is pushed to operational commanders for their use.

Retention

While it is definitely useful to have some cyber-experienced enlisted leaders, the Air Force must consider return on investment and the value of continued technical experience and development of expertise over time. With the current model of enlisted force management, as non-commissioned officers (NCO) progress through the ranks, complete varying levels of training, and gain operational experience, their ability to progress in terms of technical skill is capped as they reach Senior NCO and must transition to leadership positions to be promotable. This means the Air Force is inherently limited in the amount of cyber skill its ISR forces can attain and often loses this technical skill to management at its apex. The unit interviews echo this concern from the Airman-perspective noting their desire to be able to continue work at a technical level and not lose promotion potential.

One solution that addresses the member-desire to stay technical, enables long-term expertise development and defined career paths, and could decrease the pay gap competition is the creation of a technical warrant officer career field for cyber operations. The Congressional Budget Office studied Warrant Officers across the services and noted considerable flexibility in law, allowing each service to use these warrant officers in different ways to meet specific technical needs.[70] In most cases, Warrant Officers come from the enlisted ranks at a certain level of experience, and stay in that specific skill set as Warrant Officers. These officers do not broaden in the types of assignments they receive, instead they are able to serve in repetitive assignments in their specialty.[71]

In applying Warrant Officers to Air Force cyber, several potential models emerge. One model would be to create one Air Force cyber warrant officer specialty and feed it from the most technically capable 1N and 1B cyber personnel. This would enable the continued development of experience and create a cadre of seasoned veterans that can lead operations and mentor and train developing personnel. Another model would call for two separate warrant officer career fields, one fed from 1N personnel, and one from 1B personnel. An additional consideration for either model would be the inclusion of direct accession warrant officers. This feature may be attractive to individuals from the civilian workforce with commercial technical experience and provide new perspectives and frames of thinking. Retention has been strong across services that employ Warrant Officers with the majority serving until retirement eligible, and 50 percent of Navy Warrant Officers serving at least 24 years, and 35 percent of Army and Marine Corps Warrant Officers serving at least 24 years.[72]

Regardless of any specific solutions, the Air Force must look at retention proactively for Cyber ISR Airmen. Current retention numbers do not suggest a problem, but this data is confounded by active service commitments. Admiral Rogers is worried about his ability to bring in new technical skill despite current high retention rates at the NSA. Rogers notes the flood of unfilled technology jobs across U.S. industry will push the private sector to aggressively recruit new talent, in direct competition with NSA's recruitment goals.[73] Retention of ISR Airmen in cyber certainly merits further study. A simple, recurring survey to active Cyber ISR Airmen would provide career field managers with a more accurate depiction of retention factors in the coming years so they can take appropriate action to prevent or mitigate a future manning crisis.

Conclusion

ISR Airmen are indispensable to the Department of Defense's cyber missions to include national-level computer exploitation and supporting Combatant Commands via the Department's Cyber Mission Force construct. A review of policy and research combined with expert interviews resulted in the identification of shortfalls within the areas of organizational structure, training and retention ISR Airmen in cyber operations. This review allowed for multiple recommendations to address these shortfalls, most notably the recommendations of specializing the 14N career field and of creating an Air Force Warrant Officer career field as the best method to develop and retain cyber warriors able to deliver a competitive advantage to the Nation.

Notes

1. Quoted in Eli Watkins, "5 Things We Learned From Inside the U.S. Intelligence War," *CNN,* 24 November 2015, http://www.cnn.com/2015/11/24/politics/terror-threat-intelligence-nsa

2. Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015,* (Washington, D.C.: Joint Chiefs of Staff, June 2015), 2-3, 11.

3. Ibid., 13-14.

4. United States Air Force, *Air Force Future Operation Concept: A View of the Air Force in* 2035, (Washington, D.C.: United States Air Force, September 2015), 43.

5. Department of Defense, *Cyber Operations Personnel Report: Report to the Congressional Defense Committees As Required by Public Law 111-84,* (Washington D.C.: Department of Defense, April 2011), 12-14.

6. 25th Air Force, "Cyber Combat Mission Team," and "Cyber National Mission Team." (slides depicting team composition, 2015).

7. Senate, *Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command,* 13, 113th Cong., 1st sess., 2014, 13.

8. Department of Defense, *The Department of Defense Cyber Strategy,* (Washington, D.C. : Department of Defense, April 2015), 4-5.

9. Joint Chiefs of Staff, Joint Publication 3-12 (R), *Cyberspace Operations,* 5 February 2013, JP 3-12, II-2-II-5, I-6.

10. 25th Air Force, "Intelligence, Surveillance, and Reconnaissance Role in Cyber," (slide presentation), slide 6.

11. 659th Intelligence, Surveillance, and Reconnaissance Group, "ACC Cyber Forces," (659th ISRG mission briefing slides, 20 November 2015), slide 3.

12. Colonel Matthew M. Hurley, "For and From Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance," *Air & Space Power Journal 26*, no. 6 (November-December 2012): 12-33.

13. Ibid., 13-14.

14. Frank J. Cilluffo and Joseph R. Clark, "Repurposing Cyber Command," *Parameters,* 43 no. 4, (Winter 2013-2014), 111-112.

15. U.S. Strategic Command, "U.S. Cyber Command," U.S. Strategic Command, March 2015, https://www.stratcom.mil/factsheets/2/Cyber_Command/,1.

16. Department of Defense, *The Department of Defense Cyber Strategy,* 6.

17. 24th Air Force, "24th Air Force Fact Sheet," 24th Air Force, June 2014, www.24af.af.mil/library/factsheets/, 1.

18. Ibid., 1.

19. Directorate for Organizational and Management Planning/Office of the Director of Administration and Management/Office of the Secretary of Defense, "Organization of the Department of Defense," March 2012, www.odam.defense.gov, 1.

20. The United States Intelligence Community, "Member Agencies, National Security Agency," The U.S. Intelligence Community, accessed 6 October 2015, www.intelligence.gov, 1.

21. National Security Agency, "NSA/CSS Mission, Vision, Values," National Security Agency, April 16, 2015, www.nsa.gov, 1.

22. National Security Agency, “NSA Frequently Asked Questions, Oversight,” National Security Agency, January 13, 2011, para 2.

23. National Security Agency, “Central Security Service,” National Security Agency,” October 27 2014, https://www.nsa.gov/about/central_security_service/.

24. 25th Air Force, “25th Air Force Fact Sheet,” 25th Air Force, August 5 2015, newpreview.afnews.af.mil/afisra/library/factsheets, para 2.

25. Ibid., 1.

26. 24th Air Force, “24th Air Force Fact Sheet,” 1.

27. Jared Serbu, “Air Force Aims to Turn Cyber Into a Career,” Federal News Radio, 1 March 2012, http://federalnewsradio.com/defense/2012/03/air-force-aims-to-turn-cyber-into-a-career.

28. Captain Robert M. Lee, “Disruptive by Design: Saving the Air Force Cyber Community,” SIGNAL, 1 February 2015, http://www.afcea.org/content/?q=disruptive-design-saving-air-force-cyber-community.

29. Phillip Swarts, “Need to Know, 2016: Bolstering Air Force’s Cyber Realm,” Air Force Times, 31 December 2015, http://www.airforcetimes.com/story/military/2015/12/31/need-know-2016bolstering-air-forces-cyber-realm/77762068.

30. Department of The Air Force, *AFSC 14NX Intelligence Officer Career Field Education and Training Plan*, (Washington, D.C. : Department of the Air Force, 13 February 2013, 9).

31. CMSgt Adam J. Watson, DCS-ISR Enlisted Career Field Manager, HQ USAF A2 CEM, memorandum, subject: Policy Guidance for 1N4X1X Fusion Analyst Shred Reclassification, 1 Aug 14.

32. 25th Air Force, “Cyber Combat Mission Team,” and “Cyber National Mission Team,” (slides depicting team composition, 2015), slides 1-3.

33. Julie Toso, 25 AF/NICC staff, Joint Base San Antonio Lackland, Texas, e-mail, to the author, 20 October 2015.

34. CMSgt Adam J. Watson, memorandum, subject: HAF/A2 Policy Guidance for 1N4X1X Fusion Analyst Shred Reclassification.

35. Andru Wall, “Demystifying the Title 10-Titile 50 Debate*,” Harvard Law School National Security Journal*, December 2, 2011, 121.

36. Robert Chesney, “Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate,” *The University of Texas School of Law*, Public Law and Legal Theory Research Paper Series, Number 212, 580.

37. 25th Air Force, “Intelligence, Surveillance, and Reconnaissance Role in Cyber,” (slide presentation), slide 5.

38. Interview with Squadron Commanders from the 659th ISR Group, 25th Air Force, Air Combat Command, November-December 2015.

39. Colonel Matthew M. Hurley, “For and From Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance,” 21.

40. Thomas Ricks (with guest author using Jess DeFacks –Mamm name), “Why USAF is Overdue for Reorganization,” Foreign *Policy*, 21 September 2015, http://foreignpolicy.com/2015/09/21/why-usaf-is-overdue-for-reorganization.

41. “CSAF sees Cyber, ISR as Future Major Command,” U.S. Air Force, 10 September 2015, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/616739/csaf-sees-cyber-isr-as-future-major-command.aspx.

42. Lt Gen Michael J. Basla, Chief, Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force, memorandum, subject: Air Force Guidance Memorandum 33-04 – Cyberspace Operations Badge, 17 September 2014, 1.

43. Ibid., 2.

44. TSgt Kevin Williams, "New Air Force Cyberspace Badge Guidelines Released," Air Force Space Command, 27 April 2010, http://www.afspc.af.mil/news/story.asp?id=123201868.

45. Lynn M. Scott, Raymond E. Conley, Richard Mesic, Edward O'Connell, Darren D. Medlin, *Human Capital Management for the USAF Cyber Force,* RAND Project Air Force (Santa Monica, CA: RAND, 2010), 14.

46. Department of the Air Force, *AFSC 14NX Intelligence Officer Career Field Education and Training Plan,* 17.

47. Interview with Squadron Commanders from the 659th ISR Group, 25th Air Force, Air Combat Command, November-December 2015.

48. Air Education and Training Command, *Intelligence Officer Course, Course Chart,* 9 September 2015, 1-3.

49. Interview with Company Grade 14N officers from the 659th ISR Group, 25th Air Force, Air Combat Command, December 2014.

50. 24th Air Force, "39th Information Operations Squadron," 24th Air Force, 3 January 2013, www.24af.af.mil/library/factsheets/, 1.

51. Interview with Squadron Commanders from the 659th ISR Group, 25th Air Force, Air Combat Command, November-December 2015.

52. MSgt Amanda Caldwell, HAF/A2DFM, 1N4 AFS Manager, Pentagon, to the author, e-mail, 4 November 2015.

53. Air Force Personnel Center Public Affairs, "AF Announces 23 AFSCs on Reenlistment Bonus List," U.S. Air Force, 13 March 2015, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/580475/af-announces-23-afscs-on-reenlistment-bonus-list.aspx.

54. Major Eric Stride, "The US Air Force's Critical Offensive Cyberspace Capabilities: People & Partnerships," *Cyber Compendium: Cyberspace Professional Continuing Education Course Papers*, Vol 2, Issue 1 (Spring 2015): 17-25.

55. USA Jobs, accessed 29 January 2016, https://www.usajobs.gov/GetJob/ViewDetails/426732300

56. Major Eric Stride, "The US Air Force's Critical Offensive Cyberspace Capabilities: People & Partnerships," 17-25.

57. Martin C. Libicki, David Senty, Julia Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market,* RAND National Security Research Division, (Santa Monica, CA: RAND, 2014), 1-2.

58. Air Force Instruction (AFI) 36-2107, *Active Duty Service Commitments (ADSC),* 20 April 2012, 7.

59. Major Eric Stride, "The US Air Force's Critical Offensive Cyberspace Capabilities: People & Partnerships," 17-25.

60. MSgt Amanda Caldwell, HAF/A2DFM, 1N4 AFS Manager, Pentagon, Washington D.C., email to the author, 04 November 2015.

61. U.S. Air Force 14N Career Field Management Office, *14N Career Path Tool Airmen Capabilities Management Structure, Business Rules/Lexicon and Individual Capabilities Management Codes – Oct 2015,* October 2015, 1-30.

62. Interview with Squadron Commanders from the 659th ISR Group, 25th Air Force, Air Combat Command, November-December 2015.

63. Interview with Squadron Commanders from the 659th ISR Group, 25th Air Force, Air Combat Command, November-December 2015.

64. Martin C. Libicki, David Senty, Julia Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market.* 9.

65. Jennifer J. Li, Lindsay Daugherty, *Training Cyber Warriors: What Can Be Learned From Defense Language Training?* RAND Corporation, (Santa Monica, CA: RAND, 2015), 9-21.

66. Interview with Squadron Commanders from the 659th ISR Group, 25th Air Force, Air Combat Command, November-December 2015.

67. Boe, Major Michael, D., Chief, ISR Force Management, U.S. Air Force, Pentagon, Washington, D.C., email to the author, 3-4 February 2016.

68. Wanda Y. Wade, Karen K. Rasmussen, & Wendy Fox-Turnbull, “Can Technology Be a Transformative Force in Education,” *Preventing School Failure*, 57(3), 2013, 162-170.

69. Jennifer J. Vogel, David S. Vogel, Jan Cannon-Bowers, Clint A. Bowers, Kathryn Muse & Michelle Wright, “Computer Gaming and Interactive Simulations for Learning; A Meta-Analysis,” *Journal of Educational Computing Research*, *26,* no. 3, April 2006**,** 229-243.

70. Congressional Budget Office, *The Warrant Officer Ranks: Adding Flexibility to Military Personnel Management*, (Washington, D.C.: Congressional Budget Office, February 2002), 2.

71. Ibid., 7.

72. Ibid., 39.

73. Aliya Sternstein, “ Look Who’s Worried About the NSA’s 96 Percent Retention Rate,” *Defense One*, 27 Jan 2016, http://www.defenseone.com/technology/2016/01/look-whos-worried-about-nsas-96-percent-retention-rate/125462/

Bibliography

24th Air Force, "24th Air Force Fact Sheet," June 2014, www.24af.af.mil/library/factsheets.

24th Air Force, "39th Information Operations Squadron," 3 January 2013, www.24af.af.mil/library/factsheets.

25th Air Force, "25th Air Force Fact Sheet," 5 August 2015, newpreview.afnews.af.mil/afisra/library/factsheets.

25th Air Force, "Cyber Combat Mission Team," and "Cyber National Mission Team," (slide presentation), 2015.

25th Air Force, "Intelligence, Surveillance, and Reconnaissance Role in Cyber," (slide presentation), 14 July 2015, 1-8.

659th Intelligence, Surveillance, and Reconnaissance Group, "ACC Cyber Forces," (slide presentation), 20 November 2015, 1-20.

Air Education and Training Command, *Intelligence Officer Course, course Chart,* 9 September 2015, 1-3.

Air Force Instruction (AFI) 36-2107, *Active Duty Service Commitments (ADSC),* 20 April 2012.

Air Force Personnel Center Public Affairs, "AF Announces 23 AFSCs on Reenlistment Bonus List," 13 March 2015, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/580475/af-announces-23-afscs-on-reenlistment-bonus-list.aspx.

Basla, Lt Gen Michael, J, Chief, Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force. Memorandum. Subject: Air Force Guidance Memorandum 33-04 – Cyberspace Operations Badge, 17 September 2014.

Boe, Major Michael D., Chief, ISR Force Management, U.S. Air Force, Pentagon, Washington, D.C. To the author. E-mail, 3-4 February 2016.

Caldwell, MSgt Amanda, HAF/A2DFM, 1N4 AFS Manager, Pentagon, Washington, D.C. To the author. E-mail, 4 November 2015.

Chesney, Robert, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *The University of Texas School of Law Public Law and Legal Theory Research Paper Series,* Number 212: 539-629.

Cilluffo, Frank J. and Joseph R. Clark, "Repurposing Cyber Command," *Parameters* 48, no. 4 (Winter 2013-2014): 111-118.

Congressional Budget Office, *The Warrant Officer Ranks: Adding Flexibility to Military Personnel Management*, Washington D.C.: Congressional Budget Office, February 2002, 1-58.

"CSAF Sees Cyber, ISR as Future Major Command," *U.S. Air Force,* 10 September 2015, www.af.mil/News/ArticleDisplay/tabid/223/Article/616739/csaf-sees-cyber-isr-as-future-major-command.aspx.

Department of the Air Force, *AFSC 14NX Intelligence Officer Career Field Education and Training Plan,* Washington D.C.: Department of the Air Force, 13 February 2013.

Department of Defense, *Cyber Operations Personnel Report: Report to the Congressional Defense Committees as Required by Public Law 111-84,* Washington D.C.: Department of Defense, 2011.

Department of Defense, *The Department of Defense Cyber Strategy*, Washington D.C.: Department of Defense, 2015.

Directorate for Organizational and Management Planning/Office of the Director of Administration and Management/Office of the Secretary of Defense, "Organization of the Department of Defense," March 2012, www.odam.defense.gov.

Hurley, Colonel Matthew M., "For and From Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance," *Air & Space Power Journal* 26, no. 6 (November – December 2012): 12-33.

Joint Chiefs of Staff, *Joint Publication 3-12(R), Cyberspace Operations,* 5 February 2013.

Joint Chiefs of Staff, *The National Military Strategy of the United States of America,* Washington D.C.: Joint Chiefs of Staff, 2015.

Ledgett, Richard, Deputy Director, National Security Agency. In Watkins, Eli, "5 Things We Learned From Inside the U.S. Intelligence War," *CNN,* 24 November, 2015, http://www.cnn.com/2015/11/24/politics/terror-threat-intelligence-nsa.

Lee, Captain Robert M., "Disruptive by Design: Saving the Air Force Cyber Community," *SIGNAL,* 1 February 2015, http://www.afcea.org/content/?q=disruptive-design-saving-air-force-cyber-community.

Li, Jennifer, J., and Lindsay Daugherty, *Training Cyber Warriors: What Can Be Learned From Defense Language Training?* RAND Corporation, (Santa Monica, CA: RAND, 2015), 9-21.

Libicki, Martin, C., David Senty, and Julia Pollack, *Hackers Wanted: An Examination of the Cybersecurity Labor Market,* RAND National Security Research Division, (Santa Monica, CA: RAND, 2014), 1-84.

National Security Agency, "NSA/CSS Mission, Vision, Values," 16 April 2015, www.nsa.gov.

National Security Agency, "NSA Frequently Asked Questions, Oversight," 13 January 2011, www.nsa.gov.

National Security Agency, "Central Security Service," 27 October 2014, www.nsa.gov.

Ricks, Thomas and Jess DeFacks-Mamm (guest author using pseudonym), "Why USAF is Overdue for Reorganization, *Foreign Policy* 21 September 2015, http://foreignpolicy.com/2015/09/21/why-usaf-is-overdue-for-reorganization

Scott, Lynn M., Raymond E. conley, Richard Mesic, Edward O'Connell, and Darren D. Medlin, *Human Capital Management for the USAF Cyber Force,* RAND Project Air Force (Santa Monica, CA: RAND, 2010): 1-39.

Senate. *Advance Questions for Vice Admiral Michael E. Rogers, USN, Nominee for Commander, United States Cyber Command*, 113th Cong., 1st sess., 2014, 1-45.

Serbu, Jared, "Air Force Aims to Turn Cyber Into a Career," *Federal News Radio,* 1 March 2012, http://federalnewsradio.com/defense/2012/03/air-force-aims-to-turn-cyber-into-a-career.

Sternstein, Aliya, "Look Who's Worried About the NSA's 96 Percent Retention Rate," *Defense One*, 27 January 2016, http://www.defenseone.com/technology/2016/01/look-whos-worried-about-nsas-96-percent-retention-rate/125462/.

Stride, Major Eric, "The US Air Force's Critical Offensive Cyberspace Capabilities: People & Partnerships," *Cyber Compendium: Cyberspace Professional Continuing Education Course Papers,* Vol 2, Issue 1 (Spring 2015): 17-25.

Swarts, Phillip, "Need to Know, 2016: Bolstering Air Force's Cyber Realm," *Air Force Times,* 31 December 2015, http://www.airforcetimes.com/story/military/2015/12/31/need-know-2016bolstering-air-forces-cyber-realm/77762068.

Toso, Julie, 25 AF/NICC Staff, Joint Base San Antonio Lackland, TX. To the author. E-mail, 20 October 2015.

USA Jobs, position search, accessed 29 January 2016, https://www.usajobs.gov/GetJob/ViewDetails/426732300

United States Air Force, *Air Force Future Operation Concept: A View of the Air Force in 2035,* Washington D.C.: United States Air Force, 2015.

United States Air Force 14N Career Field Management Office, *14N Career Path Tool Airmen Capabilities Management Structure, Business Rules/Lexicon and Individual Capabilities Management Codes – Oct 2015*, October 2015, 1-30.

United States Intelligence Community, "Member Agencies, National Security Agency," www.intelligence.gov.

United States Strategic Command, "U.S. Cyber Command," March 2015, www.stratcom.mil/factsheets/2/Cyber_Command.

Vogel, Jennifer J., David S. Vogel, Jan Cannon-Bowers, Clint A. Bowers, Kathryn Muse and Michelle Wright, "Computer Gaming and Interactive Simulations for Learning: A Meta-Analysis," *Journal of Educational Computing Research,* 26, no. 3 (April 2006): 229-243.

Wade, Wanda, Y., Karen K. Rasmussen and Wendy Fox-Turnbull, "Can Technology Be a Transformative Force in Education," *Preventing School Failure* 57(3), (2013): 162-170.

Wall, Andru, "Demystifying the Title 10-Title 50 Debate," *Harvard Law School National Security Journal*¸ 2 December 2011, 85-142.

Watson, CMSgt Adam, J., DCS-ISR Enlisted Career Field Manager, HQ USAF A2 CEM. To AFPC/DPSIDC. Memorandum. Subject: Policy Guidance for 1N4X1X Fusion Analyst Shred Reclassification, 1 August 2014.

Williams, TSgt Kevin, "New Air Force Cyberspace Badge Guidelines Released," *Air Force Space Command,* 27 April 2010, http://www.afspc.af.mil/news/story.asp?id=12320186.